Data processing device, in particular an electronic memory component, and encryption method related thereto

The present invention relates to a data processing device, in particular an electronic memory component, comprising a plurality of access-secured sub-areas, in particular a plurality of access-secured memory areas, each having at least one assigned parameter (a_n, a_{n-1},..., a_1, a_0), in particular address.

The present invention further relates to a method of encrypting at least one parameter (a_n, a_{n-1},..., a_1, a_0), in particular the address, of at least one access-secured sub-area, in particular at least one access-secured memory area, of at least one data processing device, in particular at least one electronic memory component.

In known methods of encrypting confidential data, such as for instance personal data, key data or otherwise sensitive data, a non-volatile memory unit can only be encrypted as a compact physical overall memory in a more or less fixed manner; this means, in other words, that access can only conventionally be denied to memories in their entirety.

This method, known from the prior art, of encrypting entire I[ntegrated] C[ircuit] areas is considered disadvantageous in view of the high cost associated therewith together with its technical complexity and lack of flexibility. For this reason, attempts are constantly being made to develop alternative methods of encrypting access-secured memory areas or other sub-areas.

If, for instance, to control a memory of the size $M = 2^i = 2^{n+1}$ with $i = n+1$ address buses precisely these address buses are encrypted over the entire address space, modification of one address bus would have the possible effect of modifying a plurality of address buses, indeed even those address buses which ensure that a physically remote memory cell is addressed.

This is not sensible for a number of a memory types, including in particular memories which are organized into areas, such as E[rasable] P[rogrammable] R[ead] O[nly]M[emory], E[lectrically]E[rasable]P[rogrammable] R[ead]O[nly]M[emory] or Flash memory. Separation of the address buses into a number of areas and subsequent independent encryption of each of the individual areas is inadequate, however, with regard to security.

Taking as basis the above-described disadvantages and shortcomings and acknowledging the outlined prior art, it is an object of the present invention so to develop a data processing device, in particular an electronic memory component, of the above-mentioned type together with an encryption method related thereto, that on the one hand the security of such devices is increased considerably and on the other hand the expense associated therewith and the technical complexity are not too great.

This object is achieved with a data processing device, in particular an electronic memory component of non-volatile nature, having the features indicated in claim 1 and by an encryption method related thereto having the features indicated in claim 6. Advantageous embodiments and expedient further embodiments of the present invention are identified in the respective dependent claims.

According to the teaching of the present invention, therefore, a completely novel approach to area-wise encryption of memory contents is provided, i.e. a new method is disclosed for encrypting access-secured memory sectors of non-volatile nature and/or other sub-sectors.

To this end, the present invention allows parts of the (address) parameters of the memory areas to be encrypted in different ways with regard to the object and/or with regard to the customer and/or with regard to the "die". This means, in other words, that some sub-areas or sectors of the address do not affect all the addresses, unlike in the prior art.

According to the invention, therefore, encryption of one access-secured sub-area, in particular an access-secured memory area, is performed while taking account of the other respectively available sub-areas, in particular memory areas. This makes it possible to encrypt each sub-area with in each case different parameters.

According to a preferred embodiment of the present invention, an unencrypted address of the form a_n, a_{n-1},..., a_1, a_0 may take the following appearance, in accordance with the above-described encryption method: $f_1(a_n)$, $f_2(f_1(a_n)+a_{n-1})$, $f_3(f_2(f_1(a_n)+a_{n-1})+ a_{n-2})$,.., $f_{n+1}(f_n(f_{n-1}(...)))$, i.e. an unencrypted address of the form a_n, a_{n-1},..., a_1, a_0 may be mapped onto $i = n+1$ (scramble) functions f_i.

In this context, it is obvious that although variation of the parameter a_n, in particular of the address parameter, may influence all the other address buses, variation of the parameter a_{n-1} does not have any influence on the most significant function $f_1(a_n)$.

It is expedient for $f_i(a)$ to be any desired one-to-one function, i.e. there are precisely 2^i plain/cipher pairs, wherein an unencrypted address a_n, a_{n-1},..., a_1, a_0 is always

transformed into a unique encrypted address a'_n, a'_{n-1},..., a'_1, a'_0. On the other hand, the function f_i itself does not have to be bijective, i.e. it does not have to be reversible.

In an advantageous further embodiment of the present invention, not all stages have to be fully performed, i.e. some functions f_i may directly reproduce the relevant address bit: $a' = a$. Alternatively or in addition thereto, the address buses may also be grouped; this may appropriately mean, inter alia, that the inputs to the functions f_i and the return values from the functions f_i may be several bits wide.

In an advantageous embodiment of the present invention,

- for EPROM memories or for EEPROM memories division into two sub-areas with functions $f_i(a_n,..., a_x)$ and $f_2(f_1(a_{x-1},..., a_0))$ is useful and

- for flash memories division into three sub-areas with functions $f_i(a_n,..., a_x)$, $f_2(f_1(a_{x-1},..., a_y))$ and $f_3(f_2(f_1(a_{y-1},..., a_0)))$ is useful.

According to a particularly inventive further embodiment, access-secured memory areas may be separately secured, i.e. boundary conditions which require a physical memory are fully utilized by the new method (the wide variety of encryptions is here limited only insignificantly).

The present invention further relates to a microcontroller, in particular a smart card controller, comprising at least one data processing device of the above-described type. Accordingly, the above-described method may preferably be built into all smart card designs, for example.

The present invention finally relates to the use of at least one data processing device, in particular at least one electronic memory component, of the above-described type in at least one chip unit, in particular in at least one smart card controller, in at least one reader I[ntegrated] C[ircuit] or in at least one crypto chipset, for example in the field of audio and/or video encryption.

As already discussed above, there are various possible ways of advantageously embodying and developing the teaching of the present invention. Reference is made, in this regard, to the claims subordinate to claims 1 and 6, and the invention will be further described with reference to examples of embodiments shown in the drawings to which, however, the invention is not restricted. In the Figures:

Fig. 1 is a schematic block diagram of an example of embodiment of the encryption method according to the present invention applied to a data processing device according to the present invention.

The encryption method according to the present invention for application in an electronic memory component is based on the idea of encrypting unencrypted addresses a_n, a_{n-1},..., a_1, a_0 of an access-secured memory area only in certain areas, i.e. in dependence on one or more further memory areas, such that encrypted addresses a'_n, a'_{n-1},..., a'_1, a'_0 are formed.

To this end, $i = n+1$ one-to-one ($\dashrightarrow 2^i = 2^{n+1}$ plain/cipher-pairs) scramble functions f_1, f_2,..., f_n, f_{n+1} are provided, such that, after mapping, the unencrypted addresses of the form a_n, a_{n-1},..., a_1, a_0 have the following appearance when encrypted by the functions f_i (c.f. Fig. 1):

$$f_1(a_n),\ f_2(f_1(a_n)+a_{n-1}),\ f_3(f_2(f_1(a_n)+a_{n-1})+a_{n-2}),\ldots,\ f_{n+1}(f_n(f_{n-1}(\ldots)))$$

This makes it possible to encrypt each sub-area with in each case different parameters.

In this context, it is obvious that although variation of the addresses a_n, a_{n-1},..., a_1, a_0 may influence all the other address buses, variation of the parameter a_{n-1} does not have any influence on the most significant function $f_1(a_n)$.

As an alternative to that illustrated in Fig. 1, not all $i = n+1$ stages have to be fully performed, i.e. some functions f_i may also directly reproduce the relevant address bit: $a' = a$.

Furthermore, the address buses may also be grouped; this may mean, inter alia, that the inputs to the functions f_i and the return values from the functions f_i may be several bits wide.

LIST OF REFERENCE NUMERALS

a_0	first unencrypted address
a_1	second unencrypted address
a_{n-1}	n^{th} unencrypted address
a_n	$n+1^{th}$ unencrypted address
a'_0	first encrypted address
a'_1	second encrypted address
a'_{n-1}	n^{th} encrypted address
a'_n	$n+1^{th}$ encrypted address
f_1	first function, in particular first scramble function
f_2	second function, in particular second scramble function
f_n	n^{th} function, in particular n^{th} scramble function
f_{n+1}	$n+1^{th}$ function, in particular $n+1^{th}$ scramble function